AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

2 Facebook Accounts:
O'keefe Wrong Doer - Facebook UID 100015440166237 - "okeefe.wrongdoer" and
LilHavz Grindhard ShineHard - Facebook UID 100006669729547 - "little.havz"

Case No. 18-960M(NJ)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B

The basis for the search under Fed. R. Crim P. 41(c) is:

- ■ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: Title 18, United States Code, Sections 2119(1), 924(c), and 2

The application is based on these facts: See attached affidavit.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

TFO Matthew Gibson, FBI
Printed Name and Title

Sworn to before me and signed in my presence:

Date: December 14, 2018

Judge's signature

City and State: Milwaukee, Wisconsin

Honorable Nancy Joseph, U.S. Magistrate Judge
Printed Name and Title

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the following Facebook Accounts associated with Okeefer Hooker and Paul E. Anderson:

NAME	FACEBOOK IDENTIFICATION -UID	FACEBOOK NAME
O'keefe Wrong Doer	100015440166237	"okeefe.wrongdoer"
LilHavz Grindhard ShineHard	100006669729547	"little.havz"

that is stored at premises owned, maintained, controlled, or operated by Facebook Inc., a company headquartered in Menlo Park, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Facebook

To the extent that the information described in Attachment A is within the possession, custody, or control of Facebook Inc. ("Facebook"), including any messages, records, files, logs, photographs, videos, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for each user ID listed in Attachment A:

(a) All contact and personal identifying information, including for user "okeefe.wrongdoer" with user id 100015440166237: full name, user identification number, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.

(b) All contact and personal identifying information, including for user "little.havz" with user id 100006669729547: full name, user identification number, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.

(c) All activity logs for the accounts and all other documents showing the users' posts and other Facebook activities;

(d) All photos and videos uploaded by those user IDs and all photos and videos, including live video feeds, uploaded by any user that have either of those users tagged in them;

(e) All profile information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;

(f) All other records of communications and messages made or received by the users, including all private messages, chat history, video calling history, and pending "Friend" requests;

(g) All "check ins" and other location information;

(h) All IP logs, including all records of the IP addresses that logged into the accounts;

(i) All records of the accounts' usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the users "liked";

(j) All information about the Facebook pages that the accounts are or were a "fan" of;

(k) All past and present lists of friends created by the accounts;

(l) All records of Facebook searches performed by the accounts;

(m) All information about the users' access and use of Facebook Marketplace;

(n) The types of service utilized by the users;

(o) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

(p) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;

(q) All records pertaining to communications between Facebook and any person regarding the user or the users' Facebook accounts, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, Section 2119(1) (Carjacking) and 924(c)(brandishing a firearm in furtherance of a crime of violence) involving Okeefer Hooker, Paul Anderson, and Asia Rogers, including, for the user IDs identified on Attachment A, information pertaining to the following matters:

(a) Communications between known subjects. Communications between known subjects and unknown subjects. Pictures of clothing and gun used during armed robbery. Preparatory steps taken in furtherance of the armed robbery. Photos of vehicles involved in the armed robbery, including but not limited to, the stolen Rav4.

(b) Communications related to photos/attachments. Communications related to travel. Communications related to dates.

(c) Evidence indicating how and when the Facebook accounts were accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Facebook account owners;

(d) Evidence indicating the Facebook account owners' states of mind as it relates to the crime under investigation;

(e) The identity of the person(s) who created or used the user IDs, including records that help reveal the whereabouts of such person(s).

(f) The identity of the person(s) who communicated with the user IDs 100015440166237 and 100006669729547 regarding matters relating to the aforementioned violations of the United States Code.

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Matthew Gibson, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. This affidavit is in support of an application for a search warrant for information associated with certain Facebook user IDs that are stored at premises owned, maintained, controlled, or operated by Facebook Inc. ("Facebook"), a social networking company headquartered in Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Facebook to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the user IDs.

2. I have over 26 years of experience as a law enforcement officer and am currently assigned to the Milwaukee FBI Violent Crime Task Force as a Deputized Federal Task Force Officer. I was a Special Agent with the Federal Bureau of Investigation for over 23 years and have been an Investigator with the Milwaukee County District Attorney's Office since June of 2015. I have participated in numerous complex narcotics, money laundering, violent crime, armed bank robbery, and armed robbery investigations in violation of Title 21, United States Code, Sections 841(a)(1), 843(b) and 846, and Title 18, United States Code, Sections 924(c), 1951, 1956, 1957, 2113, 2119 and other related offenses. I have employed a wide variety of investigative

techniques in these and other investigations, including but not limited to, the use of informants, wiretaps, cooperating defendants, recorded communications, search warrants, surveillance, interrogations, public records, DNA collection, social-networking site reviews, and traffic stops. I have also received formal training regarding many of these investigative methods. As a Federal Task Force Officer, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

3. Asia S. Rogers, Okeefer D. Hooker, and Paul E. Anderson, are subjects in the armed motor vehicle robbery (carjacking) of a victim at 5916 North 61st Street, Milwaukee, Wisconsin on August 15, 2018, in violation of Title 18, United States Code, Sections 2119(1), 924(c), and 2. This affidavit is intended to show that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. There is also probable cause to search the information described in Attachment A for evidence of these crimes and contraband or fruits of these crimes, as described in Attachment B.

4. More specifically, I seek authorization to search Facebook's records, data, and information associated with Okeefer D. Hooker and Paul E. Anderson:

NAME	FACEBOOK IDENTIFICATION	FACEBOOK NAME
O'keefe Wrong Doer	100015440166237	"okeefe.wrongdoer"
LilHavz Grindhard ShineHard	100006669729547	"little.havz"

PROBABLE CAUSE

5. On August 15, 2018, at approximately 3:05 p.m., the victim parked her vehicle, a dark blue 2014 Toyota Rav4 bearing Wisconsin license plate 851-YXG, at 5919 North 61st Street in Milwaukee. The victim saw two black males and one black female walking south on the eastside of the street. The victim exited her car and walked to the east side of the street. When the subjects were close to the victim, one of the males demanded her car keys. The victim turned to face the subject and saw him pointing a black semi-automatic pistol at her head. The victim gave the keys to the subject and the victim fled on foot while the subjects took the vehicle. The victim's iPhone and gray Michael Kors wallet were in the car when it was stolen. The victim provided the following description of the subjects to officers: Subject#1 was described as a black male, approximately 5'9" tall, early 20's, approximately 150 pounds, slim build, with a low haircut or possibly bald head, wearing a black t-shirt, blue jeans, and armed with a black semi-automatic pistol; Subject#2 was described as a black male, wearing a dark t-shirt, and possibly dark pants; and Subject#3 was described as a black female, heavier set, with long hair, wearing a yellow and possibly orange t-shirt and possibly blue jeans.

6. Surveillance video from a doorbell camera from a residence at 5919 N. 61st Street shows two black males and a black female wearing clothing that matched the description provided by the victim. The footage shows the three people walking in the area immediately prior to the armed robbery/carjacking.

7. Officers obtained information that allowed them to track the stolen Rav4. At approximately 3:45 p.m., officers observed the vehicle parked in the area of 10th and

Clark Streets in Milwaukee bearing license plate ACF1693. Officers observed a heavy set black female wearing yellow clothing and carrying a purse enter the passenger side of the vehicle. The vehicle then drove off and officers lost sight of the vehicle.

8. At approximately 4:05 p.m., officers located the Rav4 parked unoccupied in front of 1940 South 32nd Street, Milwaukee, WI. Officers observed a black female wearing a yellow shirt and a black male wearing a dark shirt walking away from the area where the car was parked. They fit the description of the robbery suspects and the female appeared to be the same woman seen getting into the Rav4 at approximately 3:45 p.m.

9. At approximately 4:10 pm, Milwaukee Police Officers stopped Asia S. Rogers and Okeefer Hooker at 1931 South 33rd Street. As officers approached, Rogers was holding a cell phone and dropped a tan purse. Next to Rogers' purse, officers located the carjacking victim's gray Michael Kors wallet. Inside Rogers' purse, officers recovered a loaded Taurus PT111 Millennium G2 9mm pistol with an extended clip and a gray Apple I-Phone with a broken screen in a black case. Although the Rav4 was locked, officers were able to see Hooker's Wisconsin State Identification Card on the seat through the window. A citizen witness advised that a third subject was seen just prior to Hooker and Rogers being stopped.

10. Surveillance video from a nearby business captured a third subject running in the alley just prior to Hooker and Rogers being stopped by the police. The third subject was not located however a wet blue Gucci t-shirt was recovered along the suspected path of the fleeing subject. The shirt was submitted to the Wisconsin State Crime Lab for DNA

analysis. The surveillance video also captured Hooker and Rogers being stopped by officers and Rogers dropping her purse where officers subsequently recovered it.

11. The Rav4 was processed for evidence. Hooker's fingerprint was recovered from the front driver's side door.

12. On October 1, 2018, United States Magistrate Judge William Duffin authorized the search of the two cell phones recovered when Rogers and Hooker were arrested.

13. A review of the downloaded data from the blue Metro PCS Alcatel flip style cellular telephone located a video of a subject in the front passenger seat of a vehicle holding a firearm which appears to be the same weapon seized from Rogers' purse. The subject holding the firearm appears to be Paul Anderson. Anderson removed the extended magazine from the handgun and a cartridge is visible in the magazine.

14. The Wisconsin State Crime Lab identified Paul Anderson's DNA on the blue Gucci t-shirt.

15. On November 27, 2018, an MPD Detective displayed a photo array containing a photograph of Paul E. Anderson to the victim of the above-described armed carjacking. The victim identified Anderson as the gunman in the armed carjacking.

17. Law enforcement identified Hooker's Facebook page as username "O'Keefe Wrong Doer" and Anderson's Facebook page as username "LilHavz Grindhard ShineHard." A review of the publicly available information available on these Facebook pages revealed evidence further linking Hooker and Anderson to the carjacking described above.

18. On August 12, 2018, three days before the carjacking, Hooker posted a picture of himself and Anderson in a vehicle. In that photograph, Anderson is wearing what appears to be the same blue Gucci shirt recovered on the believed flight path of the third subject.

19. A video posted on Hooker's Facebook page shows Hooker and Anderson in a residence. Hooker has an extended handgun clip protruding from his front pants pocket. The clip appears to be the same as the handgun clip recovered from Rogers' purse. In addition, in the video, Anderson is wearing what appears to be the same blue Gucci shirt recovered on the believed flight path of the third subject.

20. As described below, Facebook maintains additional information on its servers beyond that which is publicly accessible. Given the publicly available information connecting Hooker and Anderson with the criminal conduct under investigation here, there is probable cause to believe that Facebook's servers contain additional evidence of criminal activity related to the carjacking at issue.

Types of Evidence Available Through Facebook

21. Affiant is aware of the common use of Facebook by criminal suspects and has examined or been involved in investigations where examinations have occurred concerning dozens of Facebook account profiles secured with the authority of search warrants or consent. Affiant has personally made or been made aware of numerous of recurring observations, made with such repeated consistency for Affiant to have come to believe them to be significantly more probable than improbable. Those observations include the commonality of suspects disclosing their pre-pay and nameless cellular

numbers in private wall posts and text messaging. Affiant is also aware of the commonality of criminal suspects to use the private messaging to orchestrate the liquidation of robbery loot, trade, rent or borrow vehicles used in commercial robberies, discuss of the commission of robberies, and disclosing their most current lodging arrangements. Further, Affiant is aware that criminal suspects often upload images and video of themselves and their co-actors wearing clothing worn in the commission of the robberies and casing visits as well as weapons and vehicles used in the crimes and of robbery loot obtained from those criminal endeavors. Facebook owns and operates a free-access social networking website of the same name that can be accessed at http://www.facebook.com. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

22. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers (for password retrieval), physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

23. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook

assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

24. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

25. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check in" to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic

locations at particular dates and times. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

26. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook's purposes, the photos and videos associated with a user's account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

27. Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to e-mail messages, are sent to the recipient's "Inbox" on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a Chat feature that allows users to send and receive instant messages through Facebook. These chat communications are stored in the chat history for the account. Facebook also has a Video Calling feature, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

28. If a Facebook user does not want to interact with another user on Facebook, the first user can "block" the second user from seeing his or her account.

29. Facebook has a "like" feature that allows users to give positive feedback or connect to particular pages. Facebook users can "like" Facebook posts or updates, as well as webpages or content on third-party (*i.e.*, non-Facebook) websites. Facebook users can also become "fans" of particular Facebook pages.

30. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

31. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as "liking" a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user's Facebook page.

32. Facebook Notes is a blogging feature available to Facebook users, and it enables users to write and post notes or personal web logs ("blogs"), or to import their blogs from other services, such as Xanga, LiveJournal, and Blogger.

33. The Facebook Gifts feature allows users to send virtual "gifts" to their friends that appear as icons on the recipient's profile page. Gifts cost money to purchase, and a personalized message can be attached to each gift. Facebook users can also send each other "pokes," which are free and simply result in a notification to the recipient that he or she has been "poked" by the sender.

34. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

35. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications ("apps") on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user's access or use of that application may appear on the user's profile page.

36. Facebook uses the term "Neoprint" to describe an expanded view of a given user profile. The "Neoprint" for a given user can include the following information from the user's profile: profile contact information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications.

37. Facebook also retains Internet Protocol ("IP") logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user's IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

38. Social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

39. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's "Neoprint," IP log, stored electronic communications, and other data retained by Facebook, which may not be publicly accessible, can indicate who has used or controlled the Facebook account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how

and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to "tag" their location in posts and Facebook "friends" to locate each other. This geographic and timeline information may tend to either inculpate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner's state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

40. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

41. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Facebook to disclose to the government copies of the records and other information (including the content of communications and location data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

42. I submit there is probable cause to believe that the Facebook accounts of Okeefer Hooker and Paul E. Anderson may contain evidence including, but not limited to, photographs or videos, location data, communication with co-conspirators, and the mobile telephone numbers used by Hooker, Anderson, and Asia Rogers in connection with the carjacking on August 15, 2018.

43. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States in the Eastern District of Wisconsin that has jurisdiction over the offense being investigated based upon the aforementioned evidence, there is probable cause to believe that Hooker, Anderson, and Rogers violated Title 18, United States Code, Sections 2119(1), 924(c), and 371 in connection with the carjacking.

44. The presence of a law enforcement officer is not required for the service or execution of this warrant.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the following Facebook Accounts associated with Okeefer Hooker and Paul E. Anderson:

NAME	FACEBOOK IDENTIFICATION -UID	FACEBOOK NAME
O'keefe Wrong Doer	100015440166237	"okeefe.wrongdoer"
LilHavz Grindhard ShineHard	100006669729547	"little.havz"

that is stored at premises owned, maintained, controlled, or operated by Facebook Inc., a company headquartered in Menlo Park, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Facebook

To the extent that the information described in Attachment A is within the possession, custody, or control of Facebook Inc. ("Facebook"), including any messages, records, files, logs, photographs, videos, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for each user ID listed in Attachment A:

(a) All contact and personal identifying information, including for user "okeefe.wrongdoer" with user id 100015440166237: full name, user identification number, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.

(b) All contact and personal identifying information, including for user "little.havz" with user id 100006669729547: full name, user identification number, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.

(c) All activity logs for the accounts and all other documents showing the users' posts and other Facebook activities;

(d) All photos and videos uploaded by those user IDs and all photos and videos, including live video feeds, uploaded by any user that have either of those users tagged in them;

(e) All profile information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;

(f) All other records of communications and messages made or received by the users, including all private messages, chat history, video calling history, and pending "Friend" requests;

(g) All "check ins" and other location information;

(h) All IP logs, including all records of the IP addresses that logged into the accounts;

(i) All records of the accounts' usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the users "liked";

(j) All information about the Facebook pages that the accounts are or were a "fan" of;

(k) All past and present lists of friends created by the accounts;

(l) All records of Facebook searches performed by the accounts;

(m) All information about the users' access and use of Facebook Marketplace;

(n) The types of service utilized by the users;

(o) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

(p) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;

(q) All records pertaining to communications between Facebook and any person regarding the user or the users' Facebook accounts, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, Section 2119(1) (Carjacking) and 924(c)(brandishing a firearm in furtherance of a crime of violence) involving Okeefer Hooker, Paul Anderson, and Asia Rogers, including, for the user IDs identified on Attachment A, information pertaining to the following matters:

(a) Communications between known subjects. Communications between known subjects and unknown subjects. Pictures of clothing and gun used during armed robbery. Preparatory steps taken in furtherance of the armed robbery. Photos of vehicles involved in the armed robbery, including but not limited to, the stolen Rav4.

(b) Communications related to photos/attachments. Communications related to travel. Communications related to dates.

(c) Evidence indicating how and when the Facebook accounts were accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Facebook account owners;

(d) Evidence indicating the Facebook account owners' states of mind as it relates to the crime under investigation;

(e) The identity of the person(s) who created or used the user IDs, including records that help reveal the whereabouts of such person(s).

(f) The identity of the person(s) who communicated with the user IDs 100015440166237 and 100006669729547 regarding matters relating to the aforementioned violations of the United States Code.